PB84-223122

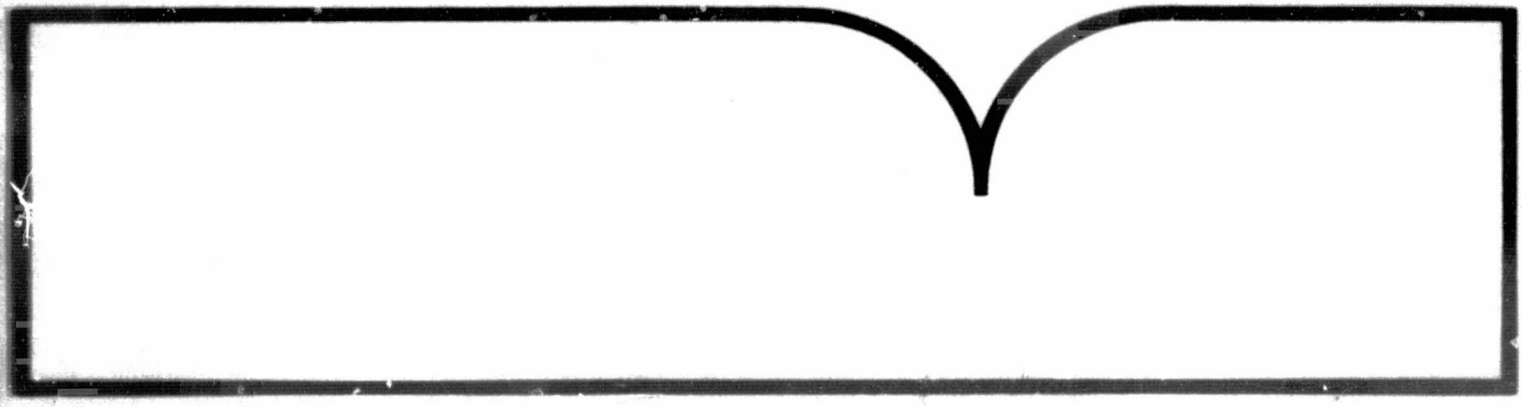
Guidelines for Certification of Existing Sensitive Systems

MITRE Corp., McLean, VA

Prepared for

National Aeronautics and Space Administration
Washington, DC

Jul 82



Guidelines for Certification of Existing Sensitive Systems

MITRE

REPORT DOCUMENTATION PAGE	1. REPORT NO.	2.	3. Recipient's Accession No. PB84 223122
4. Title and Subtitle: Guidelines for Certification of Existing Sensitive Systems			5. Report Date: July 1982 6.
7. Author(s): Paul A. Giragosiam, David W. Mastbrook, Frederick G. Tompkins			8. Performing Organization Rept. No. MTR-82W18
9. Performing Organization Name and Address: The MITRE Corporation Metrek Division 1820 Dolley Madison Boulevard McLean, VA 22102			10. Project/Task/Work Unit No. 1915C 11. Contract(C) or Grant(G) No. (C) NASW-3425 (G)
12. Sponsoring Organization Name and Address: National Aeronautics and Space Administration 400 Maryland Avenue, S. W. Washington, DC 20546			13. Type of Report & Period Covered: Final 14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

This document presents an approach for performing technical evaluations of the security of sensitive software applications. Also presented is an approach for certifying the security of applications that are currently operational. The evaluation process includes definition of security objectives, assessment of security feasibility, analysis of technical specifications and security posture evaluation. Worksheets and report formats are included. Use of threat scenario analysis teams is discussed.

17. Document Analysis a. Descriptors: Computer security, ADP security, sensitive applications, threat analysis, vulnerability analysis, security evaluation, security certification

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group

18. Availability Statement: Release Unlimited	19. Security Class (This Report): Unclassified	21. No. of Pages: 45
	20. Security Class (This Page)	22. Price

(See ANSI-Z39.18) See Instructions on Reverse OPTIONAL FORM 272 (4-77) (Formerly NTIS-35) Department of Commerce

Guidelines for Certification of Existing Sensitive Systems

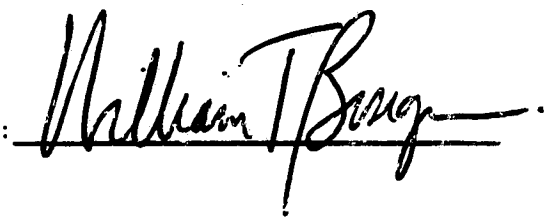
Paul A. Giragosian
David W. Mastbrook
Frederick G. Tompkins

July 1982

MTR-82W18

SPONSOR:
National Aeronautics and Space Administration
CONTRACT NO.:
NASW-3425

The MITRE Corporation
Metrek Division
1820 Dolley Madison Boulevard
McLean, Virginia 22102

MITRE Department
and Project Approval: 

ABSTRACT

This document presents pertinent information regarding the evaluation and certification of sensitive software applications in the NASA environment. The evaluation and certification of sensitive applications on a periodic basis is a sound management practice and is responsive to the requirements of OMB Circular A-71, Transmittal Memorandum No. 1. The evaluation process includes definition of security objectives, assessment of security feasibility, analysis of technical specifications, and a security posture evaluation, which includes the performance of vulnerability, threat scenario, and safeguard analyses.

TABLE OF CONTENTS

	Page
Executive Summary	ix
1. INTRODUCTION	1-1
1.1 Evaluation and Certification Action Items	1-3
1.2 Overview of the Report	1-5
2. EVALUATION AND CERTIFICATION MANAGEMENT	2-1
2.1 Roles and Responsibilities	2-1
2.2 Project Plan	2-2
3. EVALUATION PROCESS	3-1
3.1 Application Sensitivity	3-1
3.2 Security Requirements	3-1
3.2.1 Security Feasibility	3-2
3.2.2 Security Objectives	3-2
3.3 Security Technical Specifications	3-4
3.4 Security Posture Evaluation	3-5
3.4.1 Vulnerability Analysis	3-7
3.4.2 Threat Scenario Analysis	3-7
3.5 Safeguards Analysis	3-11
3.6 Evaluation Report	3-12
4. CERTIFICATION STATEMENT	4-1
APPENDIX A: THREAT SCENARIO ANALYSIS - ASSISTANCE AND CONSIDERATIONS	A-1
A.1 OUTLINE FOR INITIAL THREAT TEAM MEETING	A-2
A.1.1 Agenda	A-2
A.1.2 Primary Meeting	A-2
A.1.2 Final Meeting	A-2

TABLE OF CONTENTS

(Concluded)

	Page
A.2 SPECIFIC THREAT TEAM CONSIDERATIONS	A-3
A.2.1 Team Member Requirements	A-3
A.2.2 Avoid These Members	A-3
A.2.3 Overall Considerations	A-3
A.2.4 Advantage of the Threat Team Approach	A-3
A.2.5 Disadvantages	A-4
A.3 THREAT SCENARIO WORK SHEET	A-5
APPENDIX B: SUGGESTED EVALUATION REPORT OUTLINE	B-1
APPENDIX C: PROPOSED CERTIFICATION STATEMENT FORMAT	C-1
APPENDIX D: REFERENCES	D-1

LIST OF FIGURES

FIGURE NO.		Page
1-1	EVALUATION/CERTIFICATION PROCESS	1-4
3-1	VULNERABILITY-THREAT RELATIONSHIPS	3-8
3-2	THREAT EFFECTS AND SOURCES	3-10
3-3	SAFEGUARD EFFECTS	3-13

EXECUTIVE SUMMARY

As a part of an overall computer security effort, NASA has an on-going program to ensure the continuity of operations and data integrity of sensitive applications. OMB Circular A-71, Transmittal Memorandum No. 1, requires a periodic certification of such applications.

The purpose of this document is to provide guidance for a Center management evaluation and certification process which will evaluate the adequacy of safeguards for existing sensitive applications. The concepts presented in this report are intended to provide guidance for initial certification as well as for the recertification of existing sensitive applications. Recertification procedures will essentially be the same as certification procedures, however, they will be performed by an independent party, i.e. not the principal user. Guidance for the certification of new application systems will be addressed in a subsequent report. The procedures provided in this report may be modified by the NASA Centers to conform to their internal requirements.

Key action items for the evaluation and certification process include:

- Identification of the Degree and Scope of Application Sensitivity
- Definition of Computer Security Functional Requirements
- Definition of Computer Security Objectives
- Definition of Computer Security Technical Specifications
- Security Posture Evaluation

- Evaluation Report
- Certification Statement

The material presented in the safeguard evaluation sections of the evaluation and certification process is based on information provided in FIPS PUB 73 and FIPS PUB 65. It is recommended that the reader obtain copies of these publications for reference.

1. INTRODUCTION

A comprehensive computer security program includes several complementary areas such as: ADP facility risk analysis, personnel security, management awareness, and computer security considerations during ADP procurements.

Another aspect of an overall computer security program is an activity to ensure the continuity of operations and data integrity of sensitive applications. Central to this activity is the notion of certification for new and periodic recertification for existing sensitive applications.

OMB Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Systems," (Reference 1) contains the requirement for certification and periodic recertification of new and existing applications within the Federal sector. In addition, management instructions have been implemented NASA-wide and have established the requirement for certification of sensitive applications at each Center.

The purpose of this report is to present a guideline for a Center management evaluation and certification process which will evaluate the adequacy of safeguards for meeting the security requirements for existing sensitive applications. Certification action formally documents responsibility for the adequacy of application safeguards. Recertification will consist of identical evaluation and certification procedures performed by an independent organization. This report will discuss the major issues and concepts which form the basis for an initial certification of existing sensitive applications.

The evaluation and certification process outlined in this document will not address the following areas:

- Personnel Security. Personnel Security will be reviewed by a separate program under the NASA security office. However, the security classification of individuals associated with the sensitive application should be reviewed and any inconsistencies noted and reported to the Data Processing Installation-Computer Security Official (DPI-CSO) and the NASA security office.

- Physical Security. The physical security of the DPI and terminal locations will be addressed as part of the DPI risk analysis.

- Operating System Security. The security of the operating system will be separately reviewed. However, the sensitive application evaluation should consider password control and protection aspects.

- Privacy Act Compliance. The evaluation/certification process described herein does not specifically respond to the Privacy Act and controls relating to Privacy Act compliance will be separately reviewed. However, there may be significant overlap between this process and the review of a Privacy Act system to ensure adequate data protection.

This report makes numerous reference to material in FIPS PUB 73; FIPS PUB 65; MITRE Technical Report (MTR)-79W00445, An Overview of ADP Risk Analysis; and MTR-81W302, Security Planning for Computer Applications (References 3, 4, 5, 6). It is recommended that the reader obtain copies of these publications.

The guidance provided by this report may be modified by the NASA centers to conform to their internal procedures. The basic concepts, however, are considered an integral part of the evaluation and certification process and should not be neglected.

1.1 Evaluation and Certification Action Items

The evaluation and certification process for existing sensitive applications within NASA is illustrated in Figure 1-1. The key action items for the evaluation and certification process include:

1. Develop the Project Plan. A project plan serves as the primary management tool in directing the evaluation and certification process.

2. Identify the Degree and Scope of Application Sensitivity. Review all aspects of the application to include its attributes, features, functions, and data types to identify the degree and scope for the application.

3. Define Computer Security Functional Requirements. A user statement of requirements related to computer security is based on specific security objectives and the extent of security control automation that is feasible for the application. The test for appropriateness is related to the degree and scope of sensitivity for the application.

4. Define Computer Security Technical Specifications. A statement of specific functions or features the software should exhibit to satisfy security functional requirements. Examples include:

    - password control at the record level
    - control totals generated at specific points
    - manual review procedures

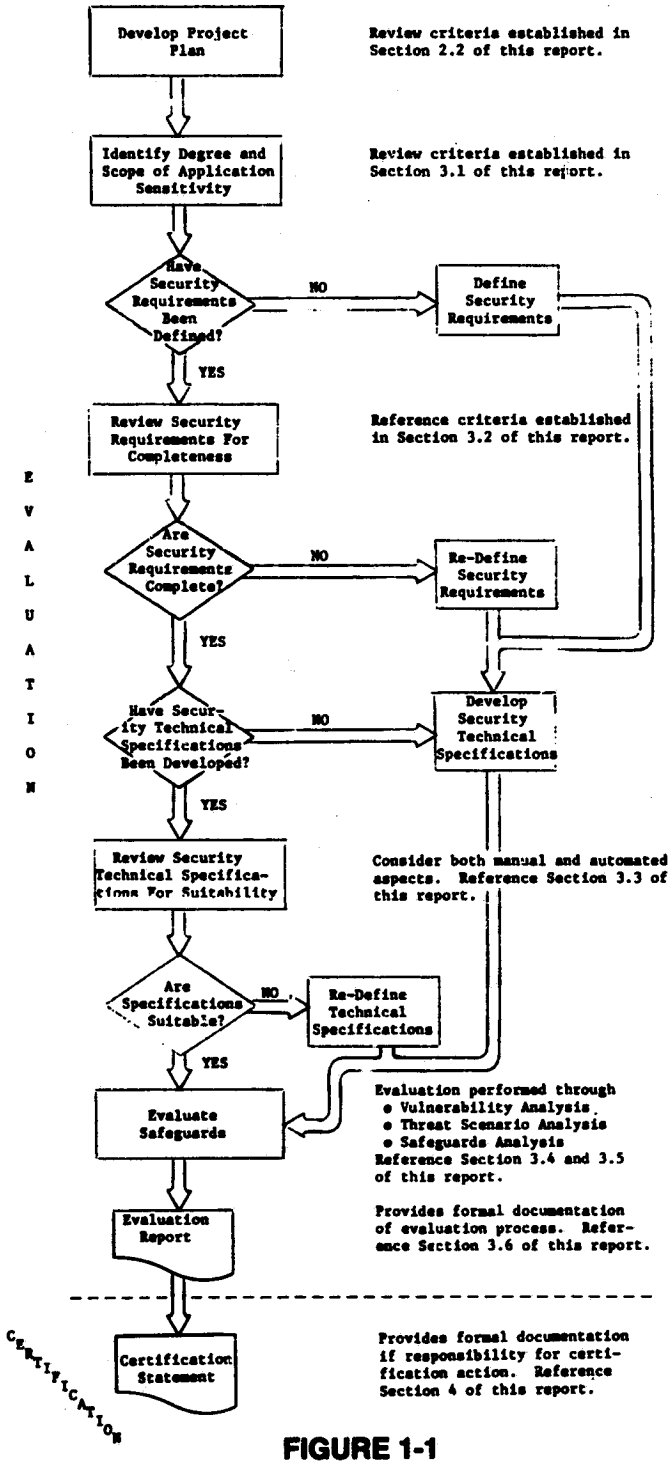


FIGURE 1-1
EVALUATION/CERTIFICATION PROCESS FOR EXISTING SENSITIVE APPLICATIONS

- check digits
- edit criteria
- limit checks

5. Evaluate Existing Safeguards. Examination of an application's vulnerabilities in conjunction with threat scenario determination provides the basis for security control evaluation. These analyses will validate the adequacy of the safeguards and isolate those instances where additional controls are required. Additional controls are developed in a safeguards analysis.

6. Evaluation Report. This report provides an overall evaluation of the control posture for the application. In addition, the report will also identify inherent weaknesses and provide recommendations for certification decision action.

7. Certification Statement. The certification statement formally documents the responsibility for initial certification of an existing application within the scope determined by the evaluation and certification process.

1.2 Overview of the Report

Section 2 of this document discusses evaluation and certification management concepts. Section 3 describes a suggested approach for the evaluation process and Section 4 presents general criteria for certification decision action.

2. EVALUATION AND CERTIFICATION MANAGEMENT

2.1 Roles and Responsibilities

The basis for certification management is provided through the NASA security management functions described in NASA Appendix J, "Computer Resources Management", NHB 2410.1. Proposed management roles and responsibilities in the evaluation and certification process are defined as follows:

Center Computer Security Official (Center CSO)

- Overall responsibility for the evaluation and certification process at the center level
- Provides assurance and guidance for performance of the project plan

Data Processing Installation Computer Security Official (DPI CSO)

- Works with the Application CSO in the development and definition of security objectives and controls
- Assumes the role of an Application CSO for those applications which have more than one primary user

Application Computer Security Official (Application CSO)

- As the primary functional user, defines project plan for the evaluation and certification process
- Determines the sensitivity of the application
- Works with the DPI CSO in the development and definition of security objectives and controls
- Signs the Certification Statement

2.2 Project Plan

The initial step in the certification management process is a project plan. The project plan serves as a management tool in directing the evaluation and certification process for an existing application and as such documents the approach taken for the evaluation process. The project plan should:

- Identify the particular application.
- Identify all baseline documentation which addresses security issues and controls. Suggested documentation includes:
  - functional requirements
  - design specifications
  - maintenance manual
  - operations manual
  - user manual
  - flow charts
  - sample I/O documents
  - management policies and procedures
- Designate roles and responsibilities of the organizations and individuals who will compose the evaluation and certification team. Typically these could include representatives from the following organizations:
  - user office
  - software maintenance
  - DPI operations
  - audit
- Define or determine the degree and scope of sensitivity
- Identify or define the security objectives
- Describe application characteristics
  - Identify application characteristics including the size and complexity

- Provide preliminary assessment of security posture. State the areas of emphasis including:

  - greatest threats, exposures, controls, etc.
  - findings of risk analysis, audits, etc.

- Provide a schedule of events for the evaluation and certification process

- Define support requirements and manpower

3. EVALUATION PROCESS

For existing systems, it may be necessary to define certain elements implicit in the overall application, but which were not reduced to writing in the early phases of the life cycle. These elements are application sensitivity, security feasibility, security objectives, and security technical requirements.

3.1 Application Sensitivity

FIPS PUB 73, Section 2.3 "Examples of Sensitive Systems", presents six application groupings which have similar security problems. The reader should review the description of security concerns for these applications. Although not exhaustive, the examples do illustrate the relationship between type of sensitivity and security objectives. In some instances, only a portion of an application system may be sensitive, i.e., the application may be sensitive only under specific circumstances or in certain operational modes. Application sensitivity may be also confined to a subsystem. Therefore, it is necessary to consider all aspects of the application. It is suggested that Appendix J, Section 502, NHB 2410.1C, be reviewed for specific NASA criteria.

3.2 Security Requirements

Verification of security requirements is based on security feasibility and security objectives for the application as discussed below.

3.2.1 Security Feasibility

For existing systems, it is necessary to review the extent of automated controls implemented within the application software or those associated with managerial or operational procedures. Section 4.3 of MTR-81W302, Security Planning for Computer Applications (Reference 6) provides general criteria for this step in the evaluation process. Specific feasibility criteria are specified in NBS FIBS PUB 73, Section 5.1, which include computer security provision for: (1) source data accuracy, (2) user identity verification, (3) restricted interfaces, (4) separation of duties, and (5) facility security. If the above criteria cannot be affirmed for the application, establishment of viable security controls by management may not be possible.

3.2.2 Security Objectives

Since the occurrence of an undesirable event during the processing of an application may result in a variety of detrimental effects, specific security objectives for the particular application must be determined. A few of these adverse events taken from NBS FIPS PUB 31, Section 1.3.2, are listed below:

- Fire
- Flood
- Power Failure
- Hardware Failure

- Intrusion
- Theft

FIPS PUB 73, Section 2, describes some general categories of security objectives and illustrates their relationship with particular types of undesirable events.

Security objectives are identified by classifying undesirable events in terms of the immediate effect rather than ultimate or final effect on data associated with the application. Examples of immediate effects of these events include:

- Modification of data
- Disclosure of data
- Unavailability of data or system services

Specific security objectives resulting from these effects are respectively:

- Data Integrity
- Data Confidentiality
- ADP Availability

Objectives may also be classified through the analysis of accidental or deliberate acts. Accidents and errors occur more frequently than deliberate acts and should receive the primary focus of attention.

It is important to remember that the implementation of a specific control in meeting a specific objective may have an

adverse effect on other objectives. If possible, security objectives must be ranked or weighted for the particular application. The determination of security objectives will also influence the security technical specifications for safeguard implementation as well as risk assessment performance.

3.3 Security Technical Specifications

Security technical specifications are determined by review of the following areas:

- Application Interfaces
- Operational Procedures
- Management Considerations
- Sensitivity and Asset Value of Data Objects
- Error Tolerance

Appropriate application documentation should be reviewed to assess the adequacy of technical specifications for security controls in these areas. Suggested action items for each of these areas are described below.

1. Application Interfaces. Identify each job component or other automated systems that provide input data to the application system or support its operation. Conversely, all job components and applications that are supported by the application system should also be identified. Review the nature of the interaction between each application job component. Suggested job components include:

   - data collection at the source

   - data entry

   - data base administration

- output dissemination

- application software maintenance

- documentation

- data archival storage

- operations

- outputs

- system programming

- internal reviews and audit procedures

- security planning and control procedures

2. Management Considerations. Identify and define the separation of duties within each job component or operational procedure as well as availability requirements for the application. Availability requirements should clearly establish limits on the maximum length of interruption for the application or its potential frequency of use.

3. Operational Procedures. Identify and define the responsibilities of the individuals who interact with the application through each interface. Constraints on use must be identified if a certain degree of security is to be enforced. This principle should also be applied to other application systems which interact with the current application. Critical operations should be identified.

4. Sensitivity of the Data Objects. Determine the sensitivity and asset value of data objects associated with the application. These data objects are the data as seen by the user rather than the data processed by the application software. Security requirements for data objects should be validated with respect to objectives of data integrity, confidentiality, availability, and fraud prevention.

5. Error Tolerance. Reliability and validity of the data and the intended objectives of the applications constitute the primary considerations in assessing the error tolerance for the application. Requirements for maintaining potential

error levels to within this tolerance must be addressed as part of the security requirements.

FIPS PUB-73 (Section 3 and Section 6.1) provides a comprehensive discussion on security controls and functional security requirements. While these examples are not exhaustive, those provided are sufficient to determine technical security specifications. The precision and method of implementation of the technical specification is influenced by the factors of security feasibility and security objectives.

3.4 Security Posture Evaluation

For those applications where security requirements have been adequately defined, an assessment of the security posture that considers the application software and its data should be performed. This assessment will include a determination of vulnerabilities and threats. The likelihood of a threat happening vs. the possible annual loss if it does occur will also be determined. Safeguards will be suggested based on the likelihood and annual loss potential. Typical vulnerabilities pertaining to threats of

- Disasters
- Delay
- Erroneous input
- Erroneous output (program errors)
- Theft
- Vandalism
- Fraud
- Information Disclosure

should be considered in the assessment. FIPS PUB 65 and MTR-79W00445, An Overview of ADP Risk Analysis (Reference 5) provides guidance in this area.

3.4.1 Vulnerability Analysis

The first step in the evaluation of controls is based primarily on the application security objectives in conjunction with inherent vulnerabilities. Together, the vulnerabilities and security objectives establish the basis for the threat scenario analysis. A vulnerability may be thought of as a 'hole' in the line of defense against threats. It is the absence or ineffectiveness of a safeguard. Threats will reduce a system's integrity, confidentiality, or availability. See Figure 3-1 for an illustration of this concept.

Although an application's vulnerability to some types of threats may vary, certain vulnerabilities are common to most sensitive applications. A detailed checklist for common types of vulnerabilities may be found in the Appendix of FIPS PUB 65. A work sheet is provided in Appendix A to help with this analysis.

3.4.2 Threat Scenario Analysis

Threat scenarios serve to validate a security control's effectiveness against an application's vulnerabilities and security requirements. A threat is a circumstance which may cause loss or harm to the system, e.g., the employment of a

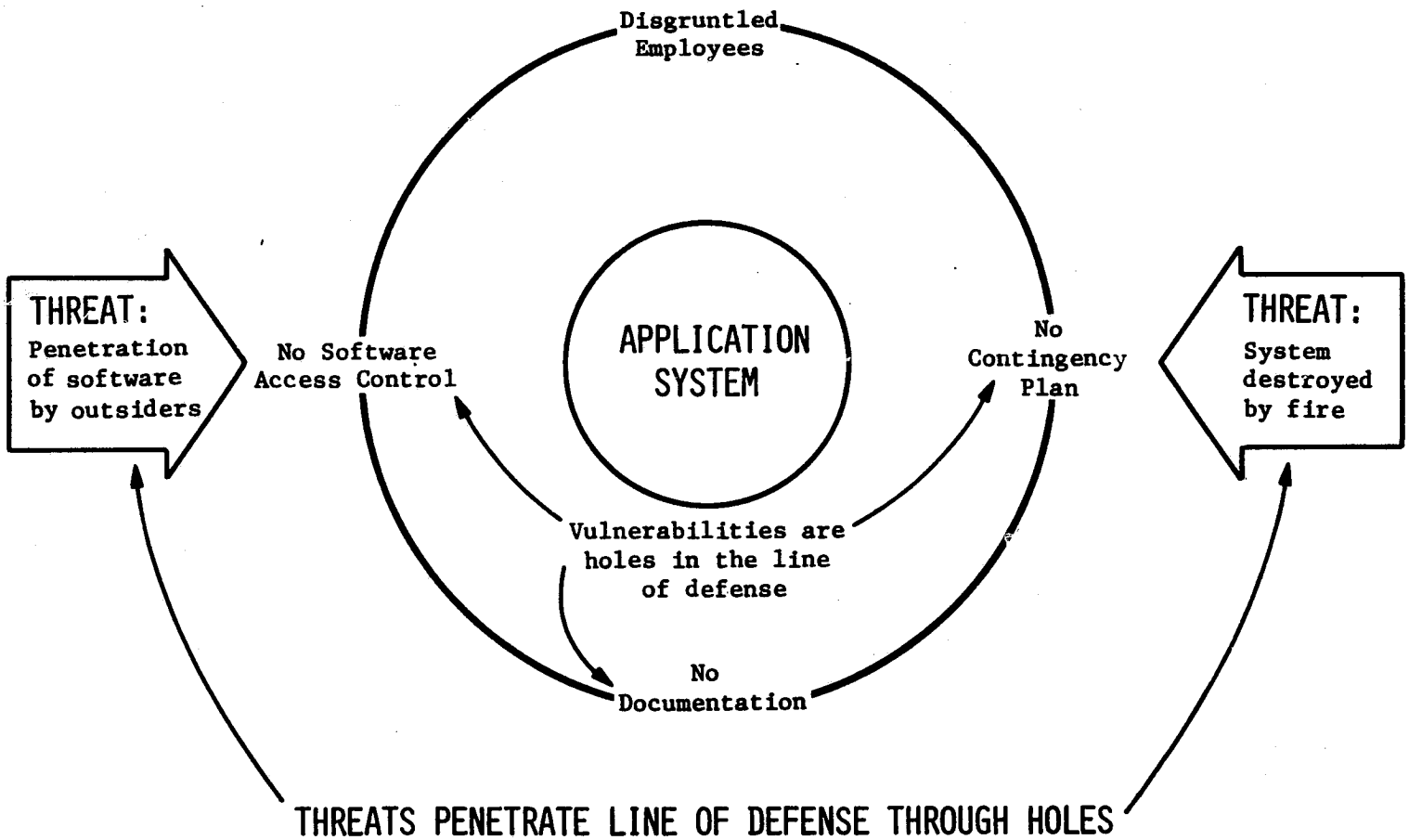


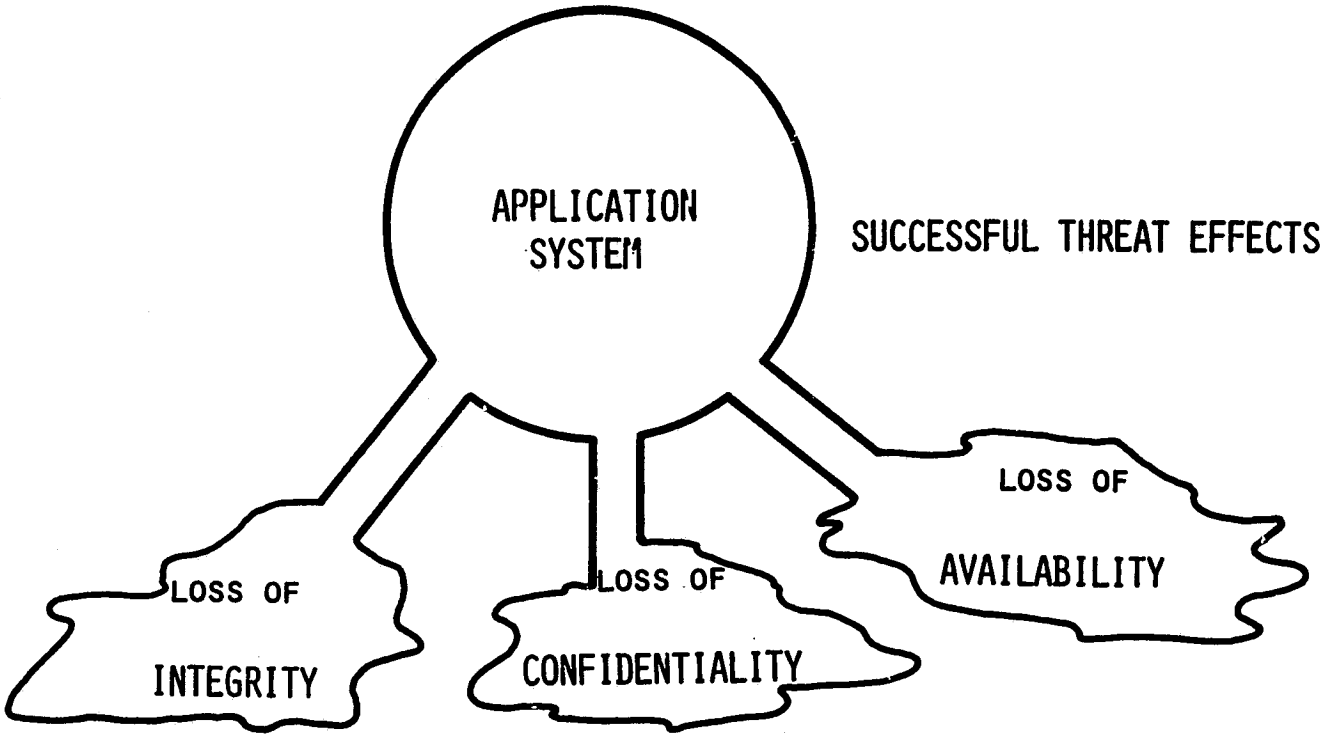
FIGURE 3-1
VULNERABILITY–THREAT RELATIONSHIPS

convicted embezzler as a bank teller. Figure 3-1 illustrates how threats penetrate defenses through vulnerabilities and Figure 3-2 illustrates the effect of successful penetration.

In addition, threat scenarios also serve to isolate those aspects of an application which lack effective safeguards. Guidance for this evaluation technique is presented in references 7 and 8.

An effective threat scenario analysis team is composed of personnel who are familiar with all aspects of the application interfaces described in Section 3.4. Not more than ten personnel should be selected for the team. Once the team members have been identified, the team leader should develop a short statement that defines those application aspects which will be considered for threat scenario analysis. The statement should also include a list of vulnerabilities and security objectives. A few possible or probable threats for the application should be provided as examples and a full meeting for the team should also be scheduled. The preliminary material should be sent to each member of the team well in advance of the first team meeting.

Actual threat scenario development is accomplished through a series of informal team meetings. Each meeting should be scheduled for a minimum of two and one-half hours. It is recommended that at least two meetings be held. Each meeting should begin with a discussion and review of preliminary material or material provided from the previous meeting. Flip charts may be used with all pages put on full display once



THREAT SOURCES

NATURAL	HUMAN	
	INTENTIONAL	ACCIDENTAL
• Fire	• Riot	• Errors
• Flood	• Sabatoge	• Omissions
• Storm	• Fraud	• Lack of Planning
• Earthquake	• Theft	• Physical Accident
	• War	

FIGURE 3-2
THREAT EFFECTS AND SOURCES

filled. Whenever possible, the team should attempt to determine the probability of a particular threat occurrence. However, if a probability cannot be immediately assigned, it is desirable to categorize the threat occurrence in general terms such as high, medium, or low. Safeguards which counter each threat should be developed by the team and listed for the threat.

Finally, the threats must be ranked. The ranking of threat scenarios may be accomplished through consensus action by the threat scenario team. See Appendix A for threat scenario worksheets.

3.5 Safeguards Analysis

Safeguards should be developed for the vulnerabilities listed in the vulnerability analysis. Use the safeguards developed in the threat scenario analysis and those developed from the vulnerability analysis to conduct the safeguard analysis. The safeguards should be ranked into three categories for implementation.

- Critical - These measures reduce a serious vulnerability to a threat. Implementation should take place immediately to establish or maintain the proper level of security.
- Necessary -These measure reduce a less serious vulnerability to a threat. This control should be implemented but the need is less immediate than for critical safeguards.
- Desirable - These measures provide extra levels of security and are discretionary.

Figure 3-3 shows how safeguards plug "holes" in the line of defense.

The ranking of safeguards using the above categories provides a basis for management decisions for an implementation time frame. A cost benefit analysis or a return on investment determination should also be done to assist in the selection of safeguards for implementation. A return on investment determination is based on the difference between the expected loss before the implementation of the safeguard, less the expected loss after the implementation of the safeguard, divided by the cost of the safeguard. In many cases obtaining quantitative data may not be feasible, and a qualitative evaluation may be necessary. In these cases, a high, medium, or low value may be used for these elements. After safeguards have been ranked and benefits assessed, recommendations for management decisions can be made.

3.6 Evaluation Report

The primary purpose of the evaluation report is to document the evaluation and subsequent certification process for an application and to serve as the basis for the certification statement. It also establishes the degree of confidence to be placed in the evaluation process and its findings.

The report should accurately reflect the existing control posture for the applications. The major portion of the findings should discuss the results obtained from the vulnerability, threat scenario, and safeguard analyses. The report will also

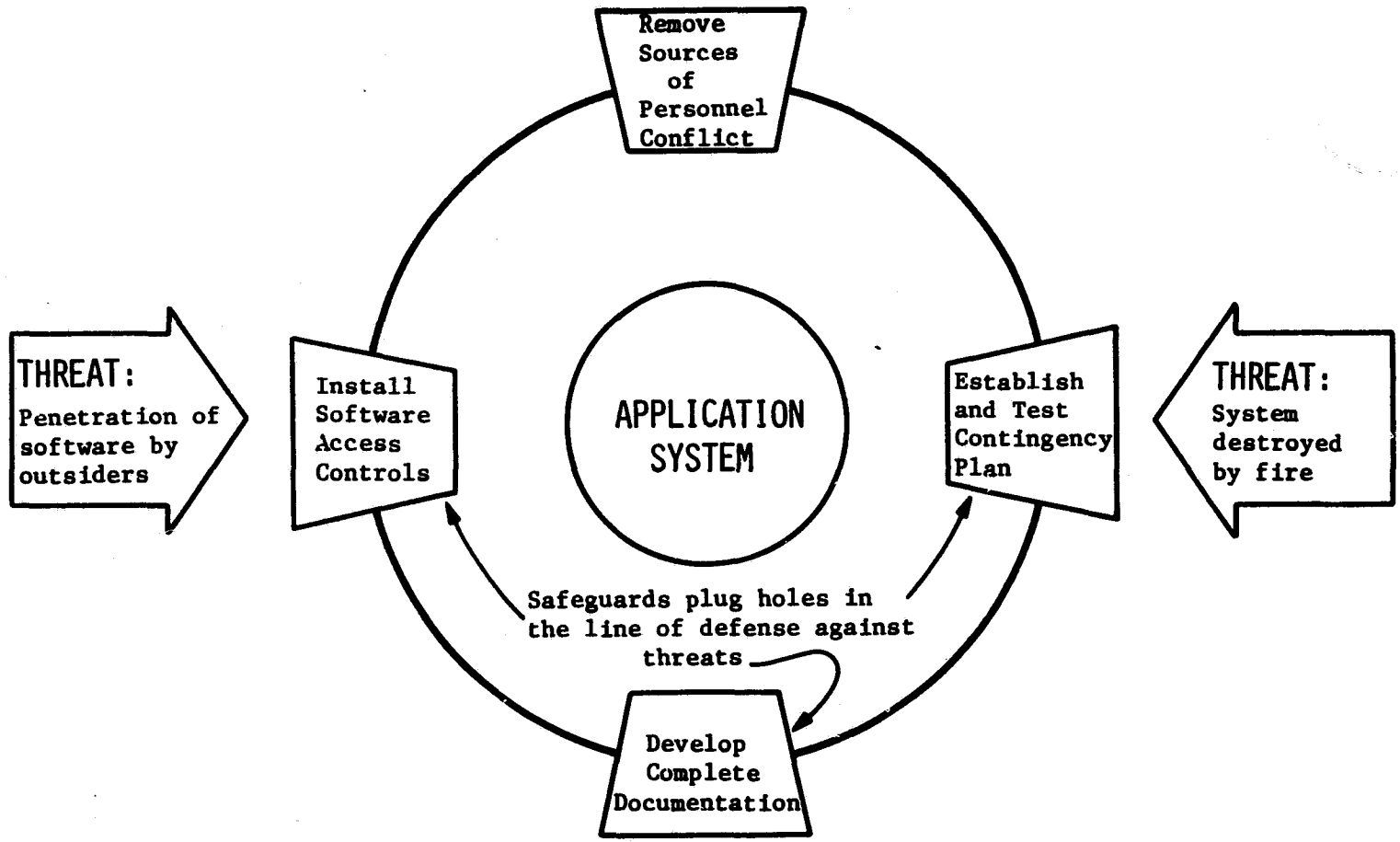


FIGURE 3-3
SAFEGUARD EFFECTS

identify any serious application shortcomings which may require further study such as a modification in operational procedures. The evaluation report is maintained in the security file for the sensitive application. A suggested outline for the evaluation report is presented in Appendix B.

4. CERTIFICATION STATEMENT

The certification statement represents the final step in the evaluation/certification process for an existing application. The Application CSO is responsible for making the certification decision. The decision process involves interpreting the recommendations made in the evaluation report and in some cases, defining controls that must be implemented in order to authorize continued operation. The decision process may be influenced by the operational impact of implemented safeguards or by increased costs incurred due to restrictions imposed on the application's functions.

Typical restrictions which may affect continued operation include:

- Addition of procedure controls
- Separation of duties
- Restriction to process data of reduced sensitivity
- Restriction on the number of user individuals
- Removal of unauthorized access in a dial-up mode by utilization of security software packages
- Removal of application subsystem or component functions software

A suggested format for the certification statement is presented in Appendix C.

APPENDIX A

THREAT SCENARIO ANALYSIS - ASSISTANCE AND CONSIDERATIONS

The following pages provide:

1. An outline for the threat team meetings.

2. Specific threat team considerations.

3. An example work sheet to help the team develop scenarios.

4. Example work sheets to help in the vulnerability, threat scenario, and safeguard analysis.

A.1 OUTLINE FOR INITIAL THREAT TEAM MEETING

A.1.1 Agenda

- Purpose of threat teams
- Steps Involved
- War Stories
- Vulnerability Analysis
- Threat Scenario Discussion
- Determine Probability of Scenario Occurrence
- Determine Ranking of Scenario
- Wrap-up and Summary

A.1.2 Primary Meeting

- Confidential, to prevent disclosure of system vulnerabilities
- Moderator uses flip charts to summarize as discussion occurs
- Alternative: Each member summarizes the scenario and turns it over to the moderator for editing and it is also summarized on-going using a flip chart for the group.

A.1.3 Final Meeting

- Meet again for one hour to go over transcript or write-up and inject second thoughts.

A.2 SPECIFIC THREAT TEAM CONSIDERATIONS

A.2.1 Team Member Requirements

- Knowledge of the System
- Confidence and personal security to allow the individual to participate without fear
- Imagination
- Outgoing personality

A.2.2 Avoid These Members

- Managers with a general overall responsibility who have little day to day contact with the specifics of the operational system.
- Persons new in their job
- Security Officers

A.2.3 Overall Considerations

- No more than 10 members for a team
- 2 to 2½ hour primary session

A.2.4 Advantage of the Threat Team Approach

- Realistic practical vulnerabilities
- Low cost
- Management awareness and interest
- Employee's willingness to participate (gaming)

- Integrates well
- Accepted by management
- Provides a basis for testing controls

A.2.5 Disadvantages

- Secrecy required (exposes weaknesses)
- Skilled leader required
- Not always methodical

EXAMPLE OF COMPLETED THREAT SCENARIO WORK SHEET

A.3 THREAT SCENARIO WORK SHEET

1. What is attacked or compromised in the system?

   The integrity of software and records.

2. What vulnerabilities allow the attack?

   Lack of passwords for files and/or lack of an overall software security package to control access.

3. What methods could be used?

   Obtain access to the system by a remote dial-up terminal. Browsing is done and various files are deleted, changed, etc.

4. What safeguards or controls can prevent the loss?

   Implementation of a software security package and modify files to require software access.

5. What is the likelihood that this scenario will work? (High, medium or Low)

   High

6. What is the impact on the assets if it does work? (Order of magnitude in dollars, i.e., tens, hundreds, thousands, etc.)

   $1,000K

Vulnerability Safeguard Summary

Vulnerabilities (A brief description)	Proposed Safeguards	Priority of Safeguards	Cost Benefit or Level of Return on Investment
1. Lack of complete written step-by-step procedures for clerks to use I/O processing.	Generate procedures	Necessary	High
2. Lack of passwords for programs and files.	Modify programs for passwords and/or provide a front-end security package for all software.	Critical	Very high
3. Incomplete documentation through the program flow chart level	Complete documentation	Desirable	Medium

Threat Scenario Vulernability Summary

Scenarios (A brief description)	Existing vulnerabilities which may be exploited	Possible loss per year	Likelihood	Rankin
Example:				
Maliciously alter someone Else's records or sabotage program and data base	Direct access to program through TSO	$1,000K	Med/ High	1
Obtain a copy of records for sale or private use	Direct access to program through TSO	$10K	High	2
Falsify records for one's advantage	Lack of data change controls	$5K	Low	3

Threat Scenario Safeguard Summary

Scenarios (A brief description)	Proposed Safeguards	Priority of Safeguards	Cost Benefit or Level of Return on Investment
Example:			
Maliciously alter someone else's records or sabotage programs and data base.	Implement a software security package	Critical	High
Obtain a copy of records for sale or private use.	Implement a software security package	Necessary	Medium
Falsify records	Institute data change controls	Desirable	Low

APPENDIX B

SUGGESTED EVALUATION REPORT OUTLINE

1. Executive Summary

2. Introduction/Background

3. Evaluation Process

    3.1 Feasibility Assessment
    3.2 Security Objectives
    3.3 Security Specifications
    3.4 Security Posture Evaluation

    3.4.1 Existing Control Posture
    3.4.2 Vulnerabilities
    3.4.3 Threat Scenario Analysis
    3.4.4 Safeguards Analysis

4. Recommendations

Attachment A: Project Plan

Attachment B: Proposed Certification Statement

Attachment C: Threat Scenario Reports

APPENDIX C

PROPOSED CERTIFICATION STATEMENT FORMAT

Based on the evaluation of (Sensitive Application) dated (Evaluation Report Date), the security safeguards are deemed adequate for the application with restrictions or clarifications noted below, and to the best of my knowledge, meet all applicable federal policies, regulations, and standards.

_____ _____

Signature Date

(Application CSO)

APPENDIX D

REFERENCES

1. OMB Circular A-71, Transmittal Memorandum No. 1, July 27, 1978.

2. NASA, Appendix J, "Computer Resources Management" NHB 2410.1.

3. National Bureau of Standards, FIPS PUB-73, Guidelines for Security of Computer Applications, June 30, 1980.

4. National Bureau of Standards, FIPS PUB-65, Guideline for Automatic Data Processing Risk Analysis, August 1, 1979.

5. Garrison, H.F., Jr., and Simpson, G.A., An Overview of ADP Risk Analysis, MTR-79W00445, The MITRE Corporation, November 1979.

6. Tompkins, F.G., Security Planning for Computer Applications, MTR-81W302, The MITRE Corporation, December 1981.

7. FitzGerald, J., "Developing and Ranking Threat Scenarios," EDPACS, September 1978.

8. Allen, Brandt, "Threat Teams: A Technique for the Detection and Prevention of Fraud in Automated and Manual Systems," Computer Security Journal, Spring 1981.